STATE OF VERMONT
Agency of Human Services (AHS)

Access Control	REVISION HISTORY:	Chapter/Number 5.03
	EFFECTIVE DATE: 10/23/08	Attachments/Related Documents:

Authorizing Signature: Cynthia D. LaWare Date Signed: 10/23/08
Cynthia D. LaWare, Secretary, Agency of Human Services

PURPOSE:
To ensure appropriate levels of security and controls are in place so that access to AHS computers and information systems is available based on pre-established rules using roles assignment and need-to-know criteria.

BACKGROUND and REFERENCES:
45 CFR 164.308(a)(4) Health Insurance Portability and Accountability Act (1996), Access Authorization, Establishment, and Modification

45 CFR 164.502(b), 164.514(d) Health Insurance Portability and Accountability Act (1996), Minimum Necessary Rule

Although HIPAA references are cited, other Vermont statutes, rules, regulations, policies, and best practices support the requirement for access controls.

DEFINITIONS:
Access Controls - Protection mechanisms that limit users' access to information and restrict their forms of access on the system to only what is appropriate for them.

Need-to-know - Approved access to, or knowledge or possession of, specific information required to carry out official duties.

Unauthorized Access - A person gains logical or physical access without permission to an information system.

Legacy Systems- applications that have exceeded a normal lifecycle and are usually technologically obsolete

SCOPE:
This document applies to all Agency Departments, Divisions and Offices hereafter referred to jointly as "department". This document also applies to contractors, business associates, and other users of departmental information systems.

STANDARDS:
Access to AHS information systems shall be granted based on a valid need-to-know that is determined by assigned official duties, intended system usage, and the HIPAA privacy "minimum necessary rule."

As a result of this policy, for the computers and information systems they control, AHS and its departments shall write procedures and enact practices to ensure the following:

- Access control procedures and guidelines shall be established and implemented to ensure that only designated individuals can access AHS information systems.

- Proper identification and supervisory approval shall be required for requests to establish and modify information system accounts.

- Account control mechanisms shall be in place and supporting procedures shall be developed, documented and implemented effectively to review, authorize, and monitor the use of time limited or temporary accounts; and to remove, disable, or otherwise secure any unnecessary or unused accounts. Written access control documentation is required for all new systems and applications.

- Supervisors and managers shall notify the IT helpdesk when employees change roles or terminate employment with AHS to discontinue access to AHS information resources.

- Each non-AHS user of an information system shall have a program sponsor that is responsible for verifying identity of the user and communicating related access control changes to the IT helpdesk.

COMPLIANCE:

It is the responsibility of the individual departments to ensure dissemination and review of this policy to all employees within their organizations and other associates as appropriate.

AHS departments with legacy systems or other extenuating circumstances must apply in writing to the AHS CIO for exceptions to this policy and include, for each information system a plan and schedule to meet the standards.

ENFORCEMENT:

The Office of the Secretary may initiate reviews, assessments or other means to ensure that policies, guidelines or standards are being followed.